ACTA ARITHMETICA
VII (1961)

Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers"

by

A. SCHINZEL (Warszawa)

In the paper [14] mentioned in the title some historical inaccuracies are committed which ought to be corrected, besides some new results strictly connected with the above paper arise, which seem to the writer worthy of mention. This is the aim of the present paper.

To begin with, as kindly pointed out by Professor P. T. Bateman, Hypothesis H coincides for the case of linear polynomials f_i with a conjecture of L. E. Dickson announced in [7]. Therefore, it is easy to see that C_1, C_2, C_7-C_{12} are consequences of Dickson's conjecture.

On the other hand, as Dickson quoted in [8], Vol. I, p. 333, V. Bouniakowsky conjectured ([1]) that if d is the greatest fixed divisor of a given irreducible polynomial $f(x)$ (with integral coefficients, the highest coefficient > 0) then the polynomial $f(x)/d$ represents infinitely many primes. This conjecture of Bouniakowsky implies Hypothesis H for the case $s = 1$ and therefore C_3 and the first part of C_6.

Now we shall deduce Bouniakowsky's conjecture from Hypothesis H. For further use we shall deduce the following stronger proposition.

C_{13}. *Let $F_1(x), F_2(x), \ldots, F_s(x), G_1(x), G_2(x), \ldots, G_t(x)$ be irreducible integer-valued polynomials of positive degree with the highest coefficient > 0. If there does not exist any integer > 1 dividing the product $F_1(x)F_2(x)\ldots F_s(x)$ for every x and if $G_j(x) \not\equiv F_i(x)$ for all $i \leqslant s$, $j \leqslant t$, then there exist infinitely many positive integers x such that the numbers $F_1(x), F_2(x), \ldots, F_s(x)$ are primes and the numbers $G_1(x), G_2(x), \ldots, G_t(x)$ are composite.*

Proof of the implication $H \to C_{13}$. Let $F_i = \Phi_i/d_i$, $G_j = \Gamma_j/e_j$, where Φ_i, Γ_i are polynomials with integral coefficients, d_i, e_j are positive integers. Let further $d = d_1 d_2 \ldots d_s$, $e = e_1 e_2 \ldots e_t$, $F = F_1 F_2 \ldots F_s$, $\Phi = \Phi_1 \Phi_2 \ldots \Phi_s$, $d = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$.

Since the polynomial F has no fixed divisor > 1, there exist integers x_i such that

$$F(x_i) \not\equiv 0 \pmod{p_i}.$$

We can assume that the polynomials F_i, G_j $(i \leqslant s, j \leqslant t)$ are algebraically coprime, because otherwise either $G_j = F_i$ or $G_j(x)$ would be composite for all sufficiently large x. We have then $(F, G_j) = 1$ $(j \leqslant t)$ and there exist polynomials $a_j(x)$, $b_j(x)$ with integral coefficients and an integer $c_j \neq 0$ such that

$$a_j(x)F(x) - b_j(x)G_j(x) = c_j\,. \tag{1}$$

Let $c = c_1c_2 \ldots c_t$. Since every polynomial possesses infinitely many prime divisors, there exist primes $q_j \nmid cde$ such that $q_j | G(y_j)$ for some integer y_j. Let $q = q_1q_2 \ldots q_t$.

In virtue of the Chinese Remainder Theorem, there exist integers z satisfying the following system of congruences

$$\begin{aligned} z &\equiv x_i \,(\operatorname{mod} p_i^{a_i+1})\,, \quad & i \leqslant s\,,\\ z &\equiv y_i \,(\operatorname{mod} q_j)\,, \quad & j \leqslant t \end{aligned} \tag{2}$$

let z_0 be any of them. Let us consider polynomials

$$f_i(x) = F_i(dqx+z_0) = \frac{\Phi_i(dqx+z_0)}{d_i}\,.$$

Since $d_i | dq$ and $\Phi_i(z_0)/d_i = F_i(z_0)$ is an integer, polynomials f_i have integral coefficients and the highest coefficient > 0. Besides, they are irreducible. We shall show that $f(x) = f_1(x) \ldots f_s(x)$ has no fixed divisor > 1.

Suppose that prime p is such a divisor. We have by (2), since $p_i^{a_i+1} \nmid d$,

$$f(0) = F(z_0) \equiv F(x_i) \not\equiv 0 \,(\operatorname{mod} p_i)\,, \qquad i \leqslant s$$

and since $q_j \nmid e$,

$$G_j(z_0) \equiv G_j(y_j) \equiv 0 \,(\operatorname{mod} q_j)\,.$$

It follows hence by (1), because $q_j \nmid c$, that

$$f(0) = F(z_0) \not\equiv 0 \,(\operatorname{mod} q_j)\,.$$

Therefore, we must have $(p, dq) = 1$.

On the other hand, by the assumption about F, there exists an integer z_p such that

$$F(z_p) \not\equiv 0 \,(\operatorname{mod} p)\,.$$

Let x_0 be a root of the congruence

$$dqx + z_0 \equiv z_p \,(\operatorname{mod} p)\,.$$

Since $(d, p) = 1$, we have

$$f(x_0) = F(dqx_0+z_0) = \frac{\Phi(dqx_0+z_0)}{d} \equiv \frac{\Phi(z_p)}{d} = F(z_p) \not\equiv 0 \,(\operatorname{mod} p)\,.$$

Our supposition about p is therefore false and the polynomials f_i satisfy the conditions of hypothesis H. Thus, there exist infinitely many integers x such that numbers $f_i(x) = F(dqx+z_0)$ are primes. Meanwhile for every x

$$G_j(dqx+z_0) = \frac{\Gamma_j(dqx+z_0)}{e_j} \equiv \frac{\Gamma_j(z_0)}{e_j} = G_j(z_0) \equiv 0 \,(\operatorname{mod} q_j)$$

then for sufficiently large x numbers $G_j(dqx+z_0)$ are composite.

Now we shall deduce

C_{14}. *For every $k > 1$ there exist infinitely many numbers m_k such that the equation*

$$\varphi(y) = m_k$$

has exactly k solutions.

Proof of the implication $H \to C_{14}$. Consider first k even, $k = 2l$, and put in H

$$f_i(x) = 2x^{2i-1}+1 \qquad (i = 1, 2, \ldots, 2l)\,, \qquad f_{2l+1}(x) = x\,.$$

The polynomials $f_i(x)$ are irreducible, their highest coefficient is > 0 and since $f_1(-1)f_2(-1) \ldots f_{2l+1}(-1) = -1$, they satisfy the conditions of Hypothesis H. Therefore, there exist infinitely many integers x such that all $f_i(x)$ are primes. Consider for such $x > 5$ the equation

$$\varphi(y) = m_k = 4x^{4l}\,. \tag{3}$$

Since x is odd $m_k \not\equiv 0 \,(\operatorname{mod} 8)$, y may have only one of the following forms: $p^a, 2p^a, 4p^a, p^aq^\beta, 2p^aq^\beta$, where p and q are primes > 2. If $a > 1$ we should have $p(p-1) | 4x^{4l}$, whence as x is prime > 5, $p = x$ and $x-1 | 4x^{4l}$, which is impossible. Therefore, there is $a = 1$ and similarly, $\beta = 1$.

$y = p$ or $2p$ is impossible since then

$$p = \varphi(y)+1 = 4x^{4l}+1 \equiv 0 \,(\operatorname{mod} 5)\,.$$

$y = 4p$ is also impossible, because then

$$p = \tfrac{1}{2}\varphi(y)+1 = 2x^{4l}+1 \equiv 0 \,(\operatorname{mod} 3)\,.$$

In the case $y = pq$ or $2pq$, we get

$$(p-1)(q-1) = 4x^{4l}\,,$$

whence

$$p = 2x^n+1\,, \qquad q = 2x^{4l-n}+1\,.$$

Since for n even $2x^n+1 \equiv 0 \,(\operatorname{mod} 3)$, it remains the only possibility

$$y = (2x^{2i-1}+1)(2x^{4l-2i+1}+1) = f_i(x)f_{2l-i+1}(x) \tag{4}$$

or

$$y = 2f_i(x)f_{2l-i+1}(x) \qquad (i = 1, 2, \ldots, l)\,.$$

Since the numbers $f_i(x)$ are primes, the $2l$ values y given by formulae (4) satisfy (3), which completes the proof for even k.

Consider now odd k, $k = 2l+3$ $(l = 0, 1, \ldots)$ and put in C_{13}

$$F_i(x) = 2x^{6i-3}+1, \quad F_{l+i}(x) = 6x^{6i-1}+1 \quad (i = 1, 2, \ldots, l),$$
$$F_{2l+1}(x) = x, \quad F_{2l+2}(x) = 6x^{6l+2}+1,$$
$$G_j(x) = 2x^{6j-5}+1, \quad G_{l+j}(x) = 2x^{6j-1} \quad (j = 1, 2, \ldots, l),$$
$$G_{2l+1}(x) = 2x^{6l+1}+1, \quad G_{2l+2}(x) = 12x^{6l+2}+1.$$

The polynomials F_i are irreducible and satisfy other conditions of C_{13}, because in view of

$$F(-1) = -5^l\cdot 7, \quad F(1) = 3^l\cdot 7^{l+1}, \quad F(2) \not\equiv 0 \pmod 7.$$

$F(x)$ has no fixed divisor >1. Since $G_j \neq F_i$ $(i, j \leqslant 2l+2)$, there exist by C_{13} infinitely many integers x such that numbers $F_i(x)$ are primes and numbers $G_j(x)$ are composite $(i, j \leqslant 2l+2)$. Observe that the numbers $2x^n+1$ are composite for all positive $n \leqslant 6l+2$, $n \neq 6i-3$, because for n even $2x^n+1 \equiv 0 \pmod 3$. Consider for x of the above kind the equation

$$\varphi(y) = m_k = 12x^{6l+2}. \tag{5}$$

By similar arguments as in case of (3), we infer that y may have only one of the following forms: $p, 2p, 4p, pq, 2pq$, where p, q are primes >2 (the possibility $y = 9q$ or $18q$ fails, because we should have then $q = \frac{1}{6}\varphi(y)+1 = 2x^{6l+2}+1$).

It cannot be $y = p$ or $2p$, because then $p = \varphi(y)+1 = 12x^{6l+2}+1$, which is composite.

The case $y = 4p$ gives

$$p = \tfrac{1}{2}\varphi(y)+1 = 6x^{6l+2}+1 = F_{2l+2}(x). \tag{6}$$

In the case $y = pq$ or $2pq$, we get

$$(p-1)(q-1) = 12x^{6l+2},$$

whence $p-1 = 2x^n$, $q-1 = 6x^{6l+2-n}$ $(0 \leqslant n \leqslant 6l+2)$ or p, q change places.

The numbers $2x^n+1$ being composite $(0 < n \leqslant 6l+2, n \neq 6i-3)$, the only two possibilities remain

1° $y = 3(6x^{6l+2}+1) = 3F_{2l+2}(x)$ or $y = 6F_{2l+2}(x)$;

2° $y = (2x^{6i-3}+1)(6x^{6(l-i)+5}+1) = F_i(x)F_{2l-i+1}(x)$ or

$$y = 2F_i(x)F_{2l-i+1}(x) \quad (i = 1, 2, \ldots, l).$$

The numbers $F_i(x)$ being primes, the $2l+2$ values y given above satisfy (5), which together with (6) gives exactly $2l+3$ solutions of (5), q. e. d.

C_{15}. *For every $k \geqslant 1$, there exist infinitely many numbers n_k such that the equation*

$$\sigma(y) = n_k$$

has exactly k solutions.

Proof of the implication $H \to C_{15}$. Put in H,

$$f_i(x) = 2(2x+1)^{2i}-1 \quad (i = 1, 2, \ldots, 2k+1), \quad f_{2k+1}(x) = x,$$
$$f_{2k+2}(x) = 2x+1.$$

The polynomials $f_i(x)$ are irreducible, their highest coefficient is >0 and since $f_1(-1)f_2(-1)\ldots f_{2k+2}(-1) = 1$, they satisfy the conditions of Hypothesis H. Therefore, there exist infinitely many integers x such that all $f_i(x)$ are primes and since $(2^x-1)/(2x+1)^{4k+4}$ tends to infinity, infinitely many of them satisfy the inequality $2^x-1 > 4(2x+1)^{4k+4}$.

Consider for any such x the equation

$$\sigma(y) = n_k = 4(2x+1)^{4k+4}.$$

Suppose that $p^\alpha | y$, $p^{\alpha+1} \nmid y$, where p is prime, $\alpha > 1$. It follows from the above equation that $\dfrac{p^{\alpha+1}-1}{p-1} \Big| 4(2x+1)^{4k+4}$.

In virtue of the theorem of Zsigmondy (cf. [8], Vol. I, p. 195), $(p^{\alpha+1}-1)/(p-1)$ has at least one prime factor of the form $(\alpha+1)k+1$. Since $\alpha+1 > 2$ and the numbers x and $2x+1$ are primes, we clearly must have

$$(\alpha+1)k+1 = 2x+1, \quad \alpha+1 = x,$$

hence

$$2^x-1 \leqslant \frac{p^x-1}{p-1} \leqslant 4(2x+1)^{4k+4},$$

which contradicts the assumption about x. The received contradiction proves that y is squarefree, and since $n_k \not\equiv 0 \pmod 3$, $n_k \not\equiv 0 \pmod 8$, y may have only one of the forms p, pq where p and q are primes, $2 < p < q$.

$y = p$ is impossible since then

$$p = \sigma(y)-1 = 4(2x+1)^{4k+4}-1 \equiv 0 \pmod 3.$$

In the case $y = pq$ we get

$$(p+1)(q+1) = 4(2x+1)^{4k+4},$$

whence

$$p = 2(2x+1)^n-1, \quad q = 2(2x+1)^{4k+4-n}, \quad 0 < n < 2k+2.$$

Since $x \equiv -1 \pmod 3$, $2(2x+1)^n-1 \equiv 0 \pmod 3$ for all odd n, it remains the only possibility

$$y = \big(2(2x+1)^{2i}-1\big)\big(2(2x+1)^{4k+4-2i}-1\big) = f_i(x)f_{2k+1-i}(x) \quad (i = 1, 2, \ldots, k).$$

Since the numbers $f_i(x)$ are primes, the k values of y given above satisfy the equation $\sigma(y) = n_k$, which completes the proof.

P. Erdös proved without any conjecture that it there exists one m_k such that the equation $\varphi(y) = m_k$ has exactly k solutions, then there exist infinitely many such m_k ([9], Theorem 4), and the analogous theorem for the equation $\sigma(y) = n_k$ (l.c., p. 12). For $k = 1$ the well-known conjecture of Carmichael states that such a number m_k does not exist and for $k > 1$ W. Sierpiński conjectured that m_k and n_k exist (cf. [9], p. 12). We have just deduced this conjecture from Hypothesis H; by more complicated arguments we could also deduce that for every pair $\langle k, l\rangle$, where $k \neq 1$, $l \geqslant 0$, there exist infinitely many numbers m such that the equation $\varphi(y) = m$ has exactly k solutions and the equation $\sigma(y) = m$ has exactly l solutions.

On page 191 paper [14] contains two historical mistakes. The theorem about the difference of arithmetical progression formed by primes, ascribed to V. Thébault was proved earlier by M. Cantor ([2]). On the other hand, the disproving of the M. Cantor conjecture about progressions formed by consecutive primes, ascribed to the writer, was made much earlier by W. H. Loud (cf. [4]).

Part of the paper [14] concerning functions $\varrho, \bar{\varrho}$ was covered to some extent by the results of H. Smith's paper [16]. It is easy to notice, that the function Δn considered by Smith is connected with function $\bar{\varrho}$ by the condition $\bar{\varrho}(\Delta n) = n-1 < \bar{\varrho}(1+\Delta n)$ and considered by him „k-tuples" just correspond „nombres k-jumeaux" of [14].

Theorem 1 of [14] follows from the table given for Δn by Smith, his results further imply the following equalities

$$
\begin{aligned}
&\bar{\varrho}(37) = \ldots = \bar{\varrho}(42) = 11\,, \quad \bar{\varrho}(43) = \ldots = \bar{\varrho}(48) = 12\,,\\
&\qquad\qquad \bar{\varrho}(49) = \bar{\varrho}(50) = 13\,,\\
&\bar{\varrho}(51) = \ldots = \bar{\varrho}(56) = 14\,, \quad \bar{\varrho}(57) = \ldots = \bar{\varrho}(60) = 15\,,\\
&\qquad\qquad \bar{\varrho}(61) = \ldots = \bar{\varrho}(66) = 16\,,\\
&\bar{\varrho}(67) = \ldots = \bar{\varrho}(70) = 17\,, \quad \bar{\varrho}(71) = \ldots = \bar{\varrho}(76) = 18\,,\\
&\qquad\qquad \bar{\varrho}(77) = \ldots = \bar{\varrho}(80) = 19\,,\\
&\bar{\varrho}(81) = \ldots = \bar{\varrho}(84) = 20\,, \quad \bar{\varrho}(85) = \ldots = \bar{\varrho}(90) = 21\,,\\
&\qquad\qquad \bar{\varrho}(91) = \ldots = \bar{\varrho}(94) = 22\,,\\
&\bar{\varrho}(95 = \ldots = \bar{\varrho}(100) = 23\,, \quad \bar{\varrho}(101) = \ldots = \bar{\varrho}(110) = 24\,,\\
&\bar{\varrho}(111) = \ldots = \bar{\varrho}(114) = 25\,,\\
&\qquad\qquad \bar{\varrho}(115) = \bar{\varrho}(116) = 26\,,
\end{aligned}
\tag{7}
$$

thus, in particular Theorems 2 and 3 of [14].

It dispenses the writer of the duty of publishing mentioned in [14] the laborious proof that $\bar{\varrho}(100) \leqslant 23$.

From formulae (7) it immediately follows that $\bar{\varrho}(x) \leqslant \pi(x)$ for $36 < x \leqslant 116$. Paper [14] contained a proof that $\bar{\varrho}(x) \leqslant \pi(x)$ for $1 < x \leqslant 132$. Owing to Smith's results, one can prove the stronger

THEOREM. *$\bar{\varrho}(x) \leqslant \pi(x)$ for $1 < x \leqslant 146$.*

Proof. It is sufficient to prove the above inequality for $132 < x \leqslant 146$. Profiting by Lemma 3 of [14] we get

$$
\begin{aligned}
\bar{\varrho}(140) &\leqslant \bar{\varrho}(114)+\bar{\varrho}(26) = 25+7 = 32 = \pi(133)\,,\\
\bar{\varrho}(146) &\leqslant \bar{\varrho}(114)+\bar{\varrho}(32) = 25+9 = 34 = \pi(141)\,,
\end{aligned}
$$

which in view of monotonicity of functions $\bar{\varrho}$ and π gives the desired result.

Analogously, as in [14], we obtain

COROLLARY. *If $x > 1, y > 1$ and if at least one of numbers x and y is $\leqslant 146$, then*

$$\pi(x+y) \leqslant \pi(x)+\pi(y)\,. \tag{8}$$

As to inequality (8), it was verified by E. Łukasiak for $1 < x, y < 1223 = p_{201}$.

H. Smith gave also in [16], numerical data concerning k-tuples for $7 \leqslant k \leqslant 15$, $q_k \leqslant 137\cdot 10^6$. One may remark, that there was omitted there 15-tuple formed by primes $17, \ldots, 73$.

As to Hypothesis H_1 of [14], we shall give the following remarks.

L. Skula noticed (written communication) that if H_1 is true, then also the intervals $[n^2+1, n^2+n]$ and $[n^2+n+1, n^2+2n]$ contain primes.

On the other hand Hypothesis H_1 is a simple consequence of the conjectures, that for all $x \geqslant 117$ there is a prime between x and $x+\sqrt{x}$ or that for all $x \geqslant 8$ there is a prime between x and $x+\log^2 x$ (cf. H. Cramér [6]). Since these conjectures hold for $x \leqslant 20{,}3\cdot 10^6$, as can be verified owing A. E. Western ([17]) and D. H. Lehmer ([11]) tables, Hypothesis H_1 holds for all $n \leqslant 4500 < 10^3\sqrt{20{,}3}$.

As to Hypothesis H_2, it was verified by A. Gorzelewski for $n \leqslant 100$.

Finally, it seems interesting to review 17 conjectures concerning primes, written out by R. D. Carmichael from Dickson's book [8]: 13 from Volume I ([3], p. 401) and 4 from Volume II ([5], p. 76). One of these conjectures ([3], 14) is already proved ([13], [15]), 3 are consequences of Hypothesis H ([3], 6, 8, 11), 2 are consequences of Hypothesis H_1 ([3], 12, 13), 4 are various modifications of Goldbach conjecture ([3], 9; [5], 1, 2, 3), 7 are false. Among these latter: 2 are mentioned in [14], Schaffler's and Cantor's conjectures ([3], 7, 10), 3 concerning Mersenne primes M_n ([3], 1, 2, 3) are wrong respectively for $n = 13, 263, 607$, one concerning primitive roots ([3], 15) was recently disproved by A. Mąkowski ([12]) and one ([5], 4) we shall disprove now.

It states, that every prime $18n \pm 1$, or else its triple, is expressible in the form $x^3 - 3xy^2 \pm y^3$. If it is true, then for all z, the form $x^3 - 3xy^2 \pm y^3$ represents at least $\pi'(\frac{1}{3}z)$ numbers $\leqslant z$ ($\pi'(x)$ is the number of primes $18n \pm 1 \leqslant x$). But this is incompatible with Siegel's theorem (cf. [10], p. 139).

References

[1] V. Bouniakowsky, *Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs*, Mém. acad. sc. St. Pétersbourg (6), Sc. math. et phys. 6 (1857), pp. 305-329.

[2] M. Cantor, *Ueber arithmetische Progressionen von Primzahlen*, Zeitschrift für Math. u. Phys. 6 (1861), pp. 340-343.

[3] R. D. Carmichael, *Review of volume I History of the theory of numbers*, Amer. Math. Monthly 26 (1919), pp. 396-403.

[4] — *Note on prime numbers*, Amer. Math. Monthly 27 (1920), p. 71.

[5] — *Review of volume II History of the theory of numbers*, Amer. Math. Monthly 28 (1921), pp. 72-78.

[6] H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*, Acta Arithm. 2 (1936), pp. 23-46.

[7] L. E. Dickson, *A new extension of Dirichlet's theorem on prime numbers*, Messenger of Math. 33 (1904), pp. 155-161.

[8] — *History of the theory of numbers*, New York 1952.

[9] P. Erdös, *Some remarks on Euler's φ function*, Acta Arithm. 4 (1958), pp. 10-19.

[10] — and K. Mahler, *On the number of integers which can be represented by a binary form*, J. London Math. Soc. 13 (1938), pp. 134-139.

[11] D. H. Lehmer, *Tables concerning the distribution of primes up to 37 millions*, 1957, mimeographed. Deposited in the UMT File.

[12] A. Mąkowski, *On a conjecture of Murphy*, Ann. Soc. Paran. Mat. (2) 3 (1960).

[13] S. S. Pillai, *On some empirical theorem of Scherk*, J. Indian Math. Soc., 17 (1927-28), pp. 164-171.

[14] A. Schinzel et W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arithmetica 4 (1958), pp. 185-208.

[15] W. Sierpiński, *Sur une propriété des nombres premiers*, Bull. Soc. Roy. des Sc., Liège, 21 (1952), pp. 537-539.

[16] H. F. Smith, *A generalisation of prime pair problem*, MTAC 11 (1957), pp. 249-254.

[17] A. E. Western, *Note on the magnitude of the difference between successive primes*, J. London Math. Soc. 9 (1934), pp. 276-278.

Reçu par la Rédaction le 14. 10. 1960

ACTA ARITHMETICA
VII (1961)

Unpublished results on number theory II
Composition theory of binary quadratic forms

by

S. Lubelski †

Edited by C. Schogt (Amsterdam)

1. This second note gives an elementary exposition of the composition of binary quadratic forms. It is shown that the classical theory [1] carries over to the case that the coefficients are taken from a (commutative) Euclidean ring [2].

Firstly, following Dirichlet and Dedekind, the forms to be compounded will be replaced by suitable equivalent ones, and it will be proved that this leads to a unique composition of the corresponding (proper) equivalence classes. In doing this, the use of quadratic congruences and, of course, of irrational numbers will be avoided. Next, a theorem on the decomposition of a given class will be deduced, and a characterization of ambiguous classes will be given. The connection in the classical case with ideal theory shall not be discussed [3].

Helpful advices were given by Dr. C. G. Lekkerkerker who also simplified the proof of theorem 5.

2. Let I be a Euclidean ring with characteristic $\neq 2$. Then in I factorization in prime elements is possible and unique, in the usual sense. The one-element will be written 1. We consider quadratic forms

$$f(x, y) = ax^2 + bxy + cy^2 \quad (a, b, c, x, y \in I),$$

[1] For the history of the subject the reader is referred to L. E. Dickson, *History of the theory of numbers*, Vol. III, New York 1934, ch. III, p. 60-79.

[2] Actually, the considerations of this note apply more generally to all principal ideal rings with characteristic $\neq 2$, which moreover are integral domains and in which the factorization property holds.

[3] It may be recalled that in that case there is a one-to-one correspondence between classes of forms and classes of ideals. See e.g. E. Landau, *Vorlesungen über Zahlentheorie*, Bd. III, Leipzig 1927, p. 187-196; B. W. Jones, *The arithmetic theory of quadratic forms*, Carus Math. Monographs, No 10 (1950), p. 153-168. See also S. Lubelski, *Über Klassenzahlrelationen quadratischer Formen in quadratischen Körpern*, Journal reine ang. Math. 174 (1936), p. 160-184.